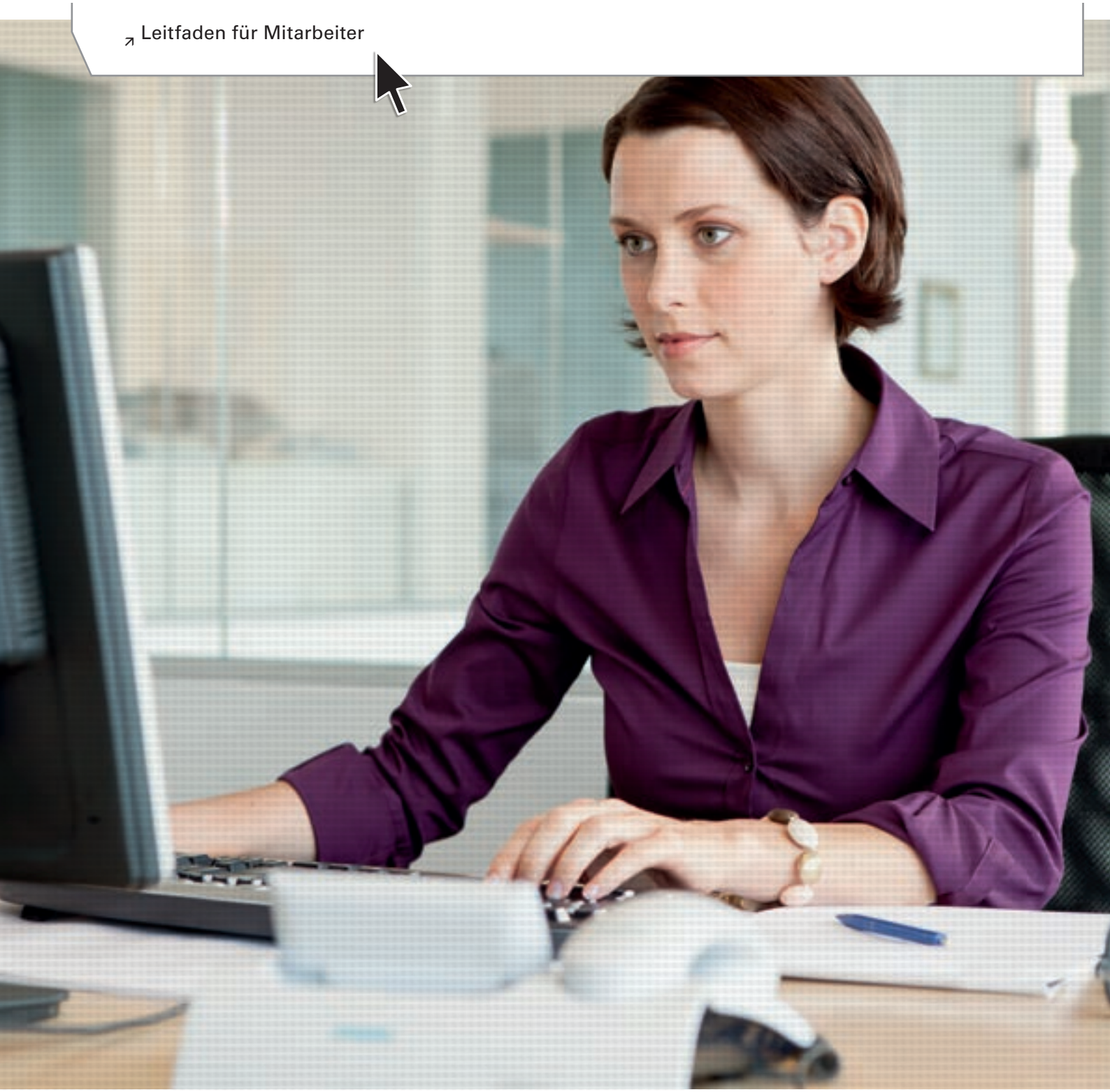
Verhaltensregeln zur Informationssicherheit

↗ Leitfaden für Mitarbeiter



↗ Eine Informationsbroschüre von DATEV und Deutschland sicher im Netz e.V.

Schirmherrschaft

Bundesministerium des Innern

DsiN.de

Vorwort

Datenverlust kann erheblichen Schaden verursachen.

Unternehmer und Mitarbeiter sollten gleichermaßen die Bedeutung von Informationen für den Erfolg eines Unternehmens kennen: In der Regel elektronisch erstellt, verarbeitet und gespeichert, sind sie seit jeher Grundlage unseres Arbeitsalltags und stellen eigenständige Unternehmenswerte dar. Informations- und Kommunikationstechnik ist heute ein fester Bestandteil der wichtigsten Geschäftsprozesse. Gehen kritische Informationen verloren oder fallen Konkurrenten in die Hände, kann das erhebliche Kosten und Wettbewerbsnachteile zur Folge haben. Auch Geschäftspartner, Kunden oder Lieferanten erwarten, dass insbesondere sensible Daten mit höchster Sorgfalt behandelt werden. Einen Datenskandal mit den damit verbundenen Imageschäden und möglichen rechtlichen Konsequenzen kann sich kein Unternehmen leisten.

In den meisten Unternehmen steht deshalb das Thema Informationssicherheit mit an oberster Stelle. In einer aktuellen Studie[1] im Auftrag des BITKOM (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.) betrachteten 74 Prozent der befragten Unternehmen Angriffe auf ihre IT-Systeme, etwa von Hackern, Konkurrenten oder ausländischen Geheimdiensten, als reale Gefahr und 30 Prozent haben sogar bereits konkrete Angriffe auf ihre IT-Systeme erlebt.

Mitarbeiter müssen für das Thema Informationssicherheit sensibilisiert sein!

Ein wirkungsvoller Schutzschild erfordert neben angemessenen technischen Sicherheitsmaßnahmen und Notfallplänen eine permanente Sensibilisierung der Mitarbeiter für das Thema Informationssicherheit. Dass Letzteres immer wichtiger ist, zeigt auch der „Sicherheitsmonitor: Mittelstand“[2] von Deutschland sicher im Netz e. V., der die IT-Sicherheitslage in Unternehmen analysiert. Laut der Studie zählt u. a. die Schulung der Belegschaft zum Thema Informationssicherheit zu den dringlichsten organisatorischen Aufgaben. Denn Bedrohungen, Risiken und Gefahren entstehen nicht nur durch Angriffe von außen auf die IT-Systeme, sondern inzwischen auch vermehrt mittels Social-Engineering-Attacken (siehe Kap. 1) oder durch die Mitarbeiter selbst (bewusst oder unbewusst). Wenn aber sorglos und nachlässig mit Daten, Programmen und Rechnern umgegangen wird, nützen technische Schutzmaßnahmen wenig.

[1] http://www.bitkom.org/de/presse/8477_78903.aspx
[2] https://www.sicher-im-netz.de/news/dsin-sicherheitsmonitor-mittelstand

Genau hier setzt dieser Leitfaden an. Er soll Sie als Mitarbeiter anhand von Praxisbeispielen auf konkrete Risiken und Gefahren in ihrem Arbeitsalltag aufmerksam machen, einen kompakten und allgemein verständlichen Überblick über das Thema Informationssicherheit geben und zu Eigenverantwortung motivieren. Konkrete Verhaltensregeln am Ende jedes Kapitels sowie Hinweise zu weiterführenden Informationen unterstützen Sie bei der Umsetzung des Gelernten und ermöglichen zugleich eine Analyse der eigenen Situation.

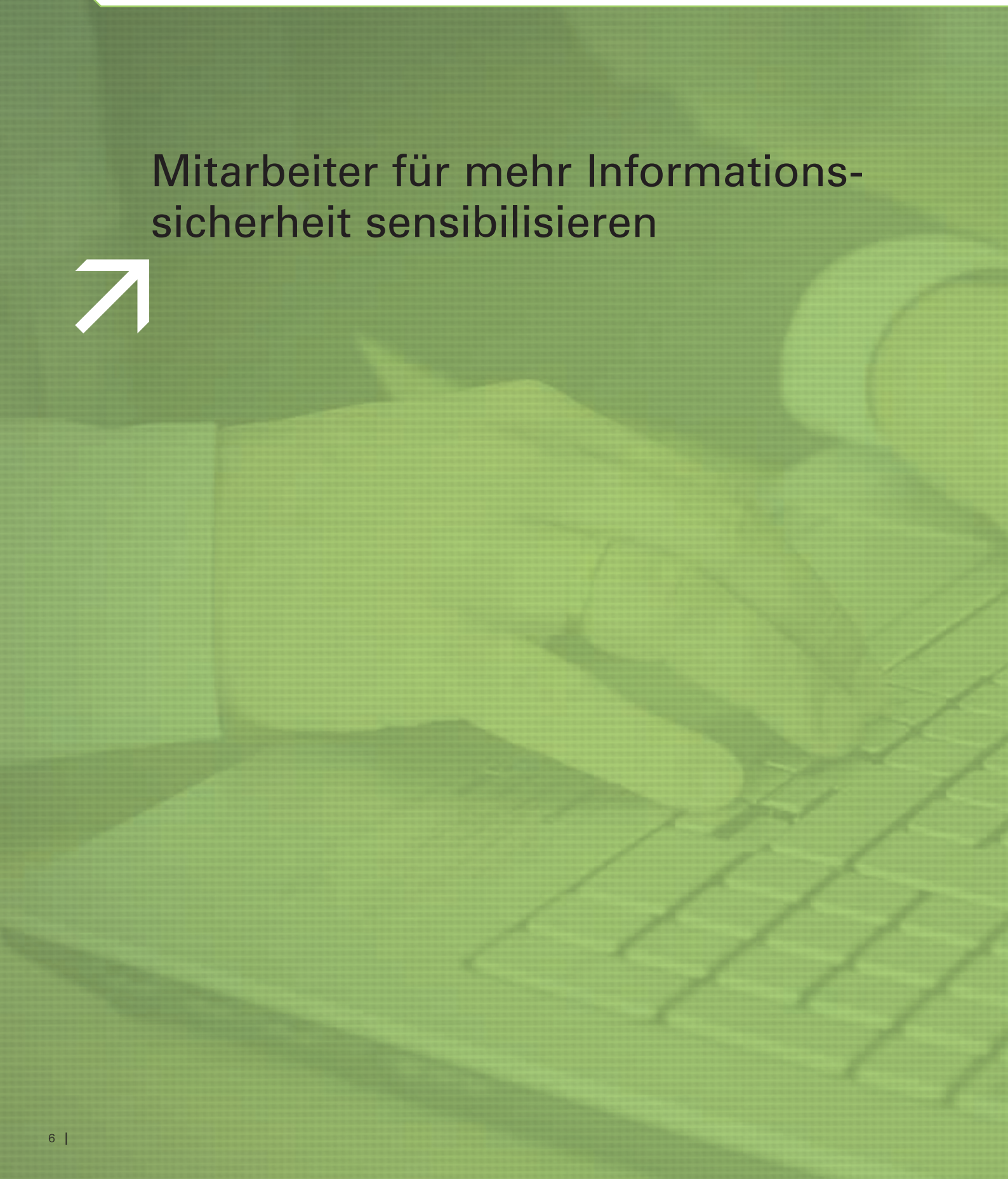
Dr. Henning Gulden
Leiter
DATEV-Gesamtsicherheitsgremium

Dr. Michael Littger
Geschäftsführer
Deutschland sicher im Netz e. V.

Verhaltensregeln zur Informationssicherheit

Leitfaden für Mitarbeiter

Mitarbeiter für mehr Informations-sicherheit sensibilisieren



Ziel dieses Leitfadens

Unternehmer und deren Mitarbeiter haben die Aufgabe, sensible Unternehmensdaten mit höchster Sorgfalt zu behandeln.

Unternehmer sollten dafür die Rahmenbedingungen schaffen, zu denen, neben technischen Schutzmaßnahmen, auch verbindliche Richtlinien in Form von klaren Sicherheitskonzepten, Regeln und Verfahrensanweisungen für alle Mitarbeiter gehören. Letztere müssen dabei verständlich kommuniziert und auch selbst täglich vorgelebt werden.

Aber Sicherheitsrichtlinien helfen nur dann, wenn sie beachtet werden, und auch die besten Sicherheitsfunktionen und -programme schützen nicht, wenn sie nicht genutzt werden. Die konsequente Berücksichtigung aller nötigen Sicherheitserfordernisse erfordert einen ständigen Lernprozess bei jedem Einzelnen und sie funktioniert erst dann nachhaltig und dauerhaft, wenn sie zur täglichen Routine wird.

Vor allem aber ist es wichtig, dass alle Mitarbeiter selbst ein grundlegendes Verständnis für Informationssicherheit aufbauen, stets mitdenken und Gefahren eigenständig einschätzen können. Denn selbst die ausgefeiltesten Sicherheitsrichtlinien können nie alle Sicherheitsaspekte des täglichen Berufslebens lückenlos abdecken.

Um ein solches grundlegendes Verständnis für Informationssicherheit zu fördern, sollten sich alle aktiv beteiligen und mit gutem Beispiel vorangehen. Denn das Thema Informationssicherheit betrifft uns alle.

Der vorliegende Leitfaden soll dabei im Rahmen von Awareness-Maßnahmen unterstützen. Je nachdem, wie intensiv man sich bereits mit dem Thema „Verhaltensregeln zur Informationssicherheit“ auseinandergesetzt hat, können die Informationen dieser Broschüre in verschiedener Weise genutzt werden. Der Leitfaden kann als Grundlage für die Entwicklung eines eigenen Sicherheits-Gesamtkonzeptes herangezogen, zur Schulung der Mitarbeiter genutzt oder auch als Nachschlagewerk und schriftliche Ergänzung zu bisherigen Sensibilisierungsmaßnahmen im Bereich Informationssicherheit eingesetzt werden.

Das Problembewusstsein für Informationssicherheit fördern und leben – dieser Leitfaden hilft dabei.

1 Social Engineering – Manipulationsversuche abwehren

Hintergrund und Risiken

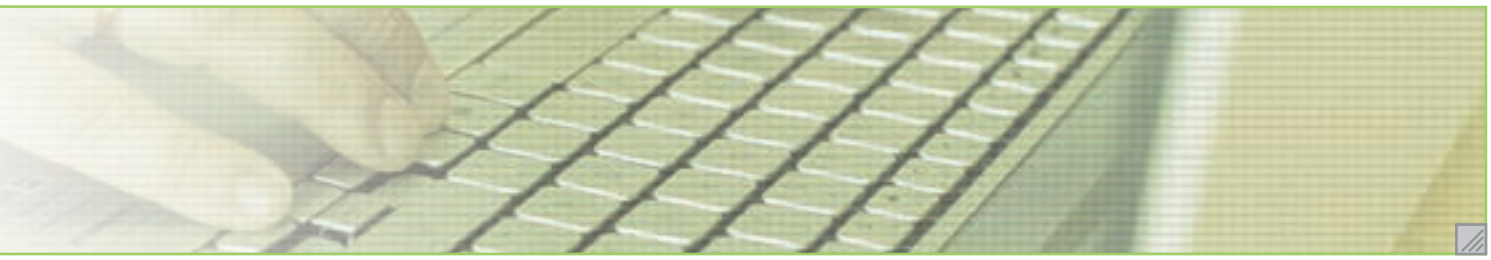
Stellen Sie sich vor, ein Mitarbeiter einer Hotline ruft Sie in Ihrem Büro an. Er benötigt von Ihnen vertrauliche Zugangsdaten, um wichtige Arbeiten abschließen zu können. Er erweckt Ihr Vertrauen mit Insiderwissen, Smalltalk über den Büroalltag und über vermeintlich gemeinsame Kollegen, er verwirrt Sie mit Fachjargon und droht Ihre Führungskraft zu kontaktieren, wenn er die geforderten Daten nicht erhält, weil Sie ihn in seiner Arbeit behindern. Was würden Sie tun?

Social-Engineering-Angriffe zielen auf menschliche Schwächen.

Das Telefongespräch ist ein beliebtes Mittel für einen sogenannten Social-Engineering-Angriff, bei dem versucht wird, Ihnen firmeninterne Informationen durch zwischenmenschliche Beeinflussung und Aushorchen zu entlocken. Diese Attacken machen sich die Hilfsbereitschaft, Gutgläubigkeit oder Unsicherheit von Mitarbeitern zunutze, um an vertrauliche Daten eines Unternehmens zu gelangen. Oft beschaffen sich die Angreifer im Vorfeld Informationen über das Umfeld des Opfers, um vertrauenswürdiger zu wirken.

Das Telefon stellt bei diesen Angriffen ein gern genutztes Medium dar, denn es ist ein vertrauter Weg der Kontaktaufnahme und kann anonym verwendet werden. Seien Sie also auf der Hut! Aber auch das Mithören von Gesprächen an öffentlichen Orten kann dazu missbraucht werden, Ihnen sensible bzw. vertrauliche Informationen zu entlocken.

Die unbedachte Weitergabe vertraulicher Daten kann Unternehmen großen Schaden zufügen. Geschäftskritische Informationen, Zugangsdaten und vertrauliche Daten von Mitarbeitern, Kunden und Lieferanten müssen stets mit höchster Sorgfalt behandelt werden. Deshalb ist ein kritischer Umgang mit Anfragen via Telefon oder E-Mail unerlässlich – ebenso wie Vorsicht bei der Weitergabe von Informationen in persönlichen Gesprächen an öffentlichen Orten, aber auch in sozialen Netzwerken!



Verhaltensregeln

- Firmenregeln: Halten Sie firmenintern vorgegebene Richtlinien immer ein, auch in Stresssituationen! Wenn es in Ihrer Firma noch keine Regeln gibt (z. B. zum Verhalten am Telefon oder zur Datenweitergabe), kontaktieren Sie die entsprechende Abteilung oder Ihre Führungskraft und bitten um die Erstellung solcher verbindlichen Richtlinien.
- Zuständigkeiten: Leiten Sie telefonische Anfragen wie z. B. Presseanfragen an die zuständige Abteilung (z. B. Public Relations) weiter bzw. verweisen Sie auf Ihre Führungskraft.
- Unbekannte: Seien Sie vorsichtig bei Ihnen unbekannten Personen und geben Sie keine internen oder vertraulichen Informationen an unbekannte Personen und unberechtigte Dritte weiter.
- Standhaft bleiben: Lassen Sie sich zu nichts überreden. Fallen Sie nicht auf Komplimente, übertriebene Höflichkeit oder Drohungen herein.
- Öffentlichkeit: Führen Sie vertrauliche Telefonate oder Gespräche nicht in der Öffentlichkeit.

Weiterführende Informationen und Links

- Einen informativen Artikel zum Thema „Social Engineering“ finden Sie auf der Seite des BSI unter folgendem Pfad: **www.bsi.bund.de > Themen > IT-Grundschutz > IT-Grundschutz-Kataloge > Inhalte > Gefährdungskataloge > G5 Vorsätzliche Handlungen > G5.42 Social Engineering**.
- Und hier können Sie sich die Informationsbroschüre „Gefahr durch Social Engineering“ herunterladen: **www.it-sicherheit.de > Ratgeber > IT-Sicherheitstipps > Sicherheit für Unternehmen > Neue Informationsbroschüre: Gefahr durch Social Engineering**.

2 Passwortdiebstahl – Medienberichte zeigen das gigantische Ausmaß

Hintergrund und Risiken

Die Arbeit am PC beginnt im Idealfall mit der Eingabe eines Passworts. Das soll den PC und das Unternehmensnetzwerk vor unbefugtem Zugang schützen. Auch Ihr E-Mail-Konto und andere Accounts werden durch Passwörter gesichert. Leider sind aber viele Menschen im Umgang mit ihren Passwörtern weit weniger vorsichtig als mit ihrem Haustürschlüssel, obwohl beide doch einem ähnlichen Zweck dienen.

Ausspionieren von Passwörtern

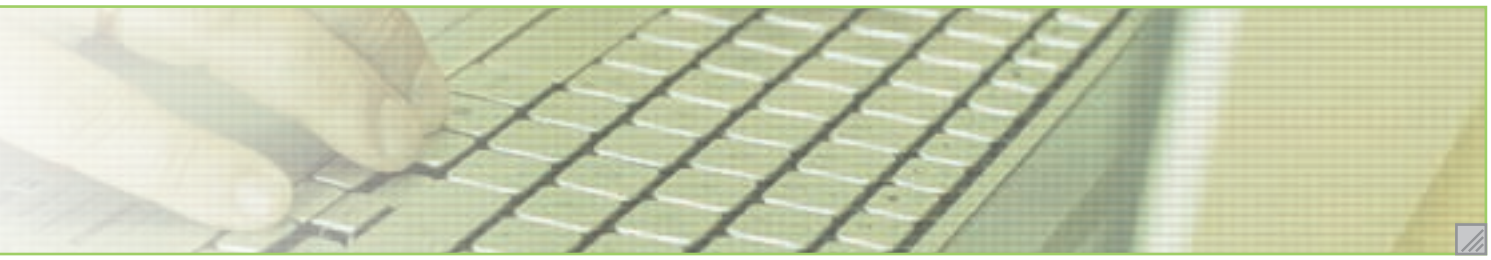
Schützen Sie Ihre wertvollen Daten mit sicheren Passwörtern.

Ein weitverbreitetes Passwort ist seit Jahren die Zahlenfolge „123456", so das amerikanische Sicherheitsunternehmen SplashData[3] in seiner alljährlichen Liste der häufigsten Passwörter. Würden Sie mit dieser Kombination auch Ihre Wohnung schützen? Mit Sicherheit nicht. Warum also sollten Sie wertvolle Daten damit sichern? Gerät ein Passwort in falsche Hände, kann das für Sie und für Ihr Unternehmen einen großen Schaden zur Folge haben (z. B. Datendiebstahl, Spam-Versand über Ihren E-Mail-Account, aber auch Interneteinkäufe in Ihrem Namen).

Es gibt zahlreiche Möglichkeiten für einen Angreifer, Ihre Passwörter auszuspionieren. Nicht immer können Sie das verhindern, wie die zahlreichen Medienberichte über Millionen gestohlener Zugangsdaten bei Online-Diensten zeigen. Aber oftmals bieten wir schon durch die Wahl unseres Passworts eine Angriffsfläche für Missbrauch. Besteht eine direkte Verbindung zum Benutzer, zum Beispiel indem das eigene Geburtsdatum oder die Namen der Kinder, des Ehepartners oder des Haustiers verwendet werden, haben Personen, die sich in Ihrem näheren Umfeld befinden oder sich anderweitig Zugriff zu diesen Informationen beschaffen können, dadurch ein leichtes Spiel.

Mit eigentlich sicheren Passwörtern wiederum wird es Angreifern nicht selten durch unbedachtes „Verstecken" von Passwortzetteln unter der Tastatur oder am Bildschirmrand besonders leicht gemacht. Auch das Über-die-Schulter-Schauen, das sog. „Shoulder Surfing", oder das Verwenden eines „Keyloggers" – eines Programms, das Ihre Tastatureingaben mitliest – sind gängige Angriffsmethoden. Weitere häufige Varianten des Passwortdiebstahls sind:

[3] http://splashdata.com/press/worstpasswords2013.htm



Brute-Force-Angriff

Bei einem Brute-Force-Angriff werden durch einen leistungsstarken PC automatisiert alle möglichen Zeichenkombinationen für ein Passwort ausprobiert. Heutzutage prüft ein durchschnittlicher PC gut mehrere Millionen Passwörter pro Sekunde. Bei einem Passwort, das nur aus einer reinen Zahlen- oder Buchstabenkombination besteht, ist eine solche Suche schnell erfolgreich. Sie sollten deshalb immer eine Kombination aus Buchstaben, Sonderzeichen und Ziffern für Ihr Passwort verwenden sowie auf eine angemessene Länge achten.

Je länger Ihr Passwort ist, desto sicherer ist es.

Wörterbuchangriff

In Wörterbuch-Attacken werden durch spezielle Programme mithilfe von umfangreichen Passwortlisten (auch Wordlists oder Dictionaries) typische Wörter und Wortkombinationen (auch aus Fremdsprachen) nacheinander getestet. Dies erfordert weniger Versuche als Brute-Force-Angriffe. Zudem macht die häufige Nutzung typischer Passwörter und bestimmter Schemata es den Angreifern besonders leicht, betroffene Accounts zu knacken.

Verhaltensregeln

- Starke Passwörter: Verwenden Sie zur Absicherung Ihrer Daten nur komplexe Passwörter, die aus Buchstaben, Ziffern und Sonderzeichen bestehen. Je mehr Zeichen Ihr Passwort hat, desto sicherer ist es. Ändern Sie Ihr Passwort regelmäßig (z. B. alle 6 Monate) und auf jeden Fall auch dann, wenn Sie glauben, dass das Passwort ausgespäht wurde.
- Diskretion: Geben Sie Ihr Passwort niemals an Dritte, insbesondere fremde Personen heraus – schon gar nicht via E-Mail oder Telefon.
- Aufbewahrung: Behalten Sie Ihre Passwörter am besten im Kopf. Benötigen Sie dennoch eine Gedächtnisstütze, achten Sie auf ausreichende Sicherheit oder nutzen Sie einen Passwortsafe: Denn Passwörter gehören nicht unter die Schreibtischunterlage oder unverschlüsselt auf Ihr Smartphone oder Ihren PC!
- Eingabe: Achten Sie bei der Passworteingabe darauf, dass niemand Sie beobachtet. Warten Sie mit der Passworteingabe, bis Sie unbeobachtet sind.

Weiterführende Informationen und Links

- Ein interessantes Video „Account-Takeover“ zur Frage „Sicherheit in sozialen Netzwerken?“ finden Sie hier Pfad: **www.justiz.nrw.de > Bürgerservice > Prävention > Film: Account-Takeover**.
- Einen informativen Artikel zum Thema E-Mail-Phishing und den Gefahren und Sicherheitsrisiken von Online-Banking finden Sie auf der Webseite des BSI. Pfad: **www.bsi-fuer-buerger.de > Wie bewege ich mich sicher im Netz? > Online-Banking > Gefahren und Sicherheitsrisiken > E-Mail-Phishing: Passwortdiebstahl mit manipulierten E-Mails**.

3 Sicheres Passwort – Gewusst wie

Hintergrund und Risiken

Passwörter sollen vor unbefugtem Zugang auf IT-Systeme und Zugriff auf Daten schützen. Ein ungeschütztes IT-System kann sowohl für Sie als auch für Ihre Firma zu erheblichen Schäden führen. Das effektive und sichere Nutzen von Passwörtern ist deshalb eine grundlegende Maßnahme, um Informationssicherheit zu gewährleisten.

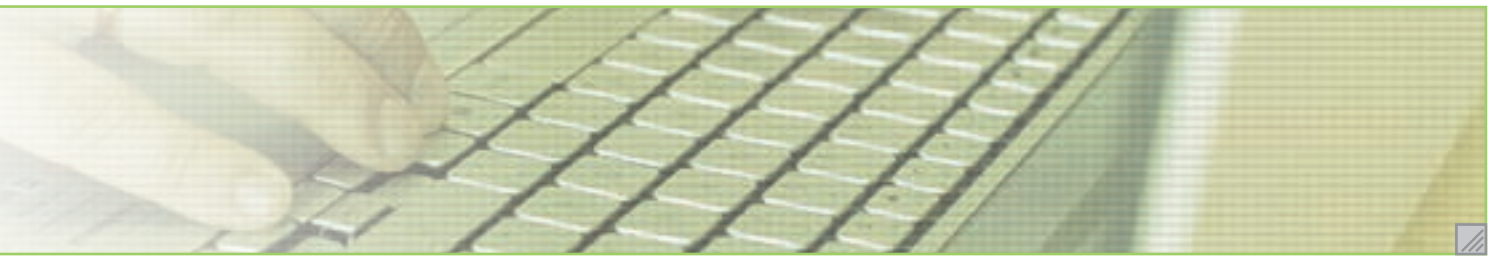
Ist Ihr Passwort sicher? Oft werden die Telefonnummer, das Lieblingsessen, der Name des Partners oder ein Geburtsdatum als Passwort verwendet – kein großes Hindernis für jemanden, der Sie kennt und sich Zugang zu Ihrem PC verschaffen möchte.

Verwenden Sie nie dasselbe Passwort bei mehreren Diensten.

Aber noch einiges mehr gilt es zu beachten. So sollten Sie kein Passwort mehrfach verwenden. Denn ist erst einmal eine Anwendung oder ein Dienst kompromittiert, was leider immer wieder vorkommt, dann wären damit auch Ihre anderen Accounts mit demselben Passwort gefährdet. Geben Sie außerdem niemals Ihr Passwort auf Webseiten ein, wenn Sie die Sicherheitseinstellungen des verwendeten Rechners nicht kontrollieren können, also zum Beispiel im Internetcafé oder am PC eines Freundes. Auch wenn Sie den Link einer Webseite in einer E-Mail erhalten haben, sollten Sie dort keinesfalls ein Passwort eingeben: Die Gefahr ist groß, dass es sich dabei um eine Phishing-Mail handelt.

Ein sicheres Passwort

- hat eine angemessene Länge von 8 Stellen, besser 10 bis 15 Zeichen – je mehr Zeichen desto besser,
- enthält sowohl Buchstaben (keine Umlaute) als auch Ziffern (0–9),
- enthält Groß- und Kleinbuchstaben und Sonderzeichen (z. B. #,$),
- enthält keine personenbezogenen Daten (z. B. Name des Haustiers),
- ist in keinem deutschen oder Fremdwörterbuch enthalten,
- wird in regelmäßigen Abständen (z. B. alle 6 Monate) geändert. Verwenden Sie bei der Erstellung neuer Passwörter keine bereits einmal genutzten Passwörter.



So merken Sie sich Ihr Passwort leicht!

Starke Passwörter entstehen durch außergewöhnliche Zeichenkombinationen, müssen aber nicht unbedingt kompliziert sein, wie Sie an den folgenden Methoden und Beispielen sehen können:

Akronymmethode

Denken Sie sich einen Satz aus und benutzten Sie von jedem Wort nur den 1. Buchstaben (oder nur den 2., den letzten etc.). Anschließend werden bestimmte Buchstaben in Zahlen oder Sonderzeichen verwandelt.
Beispiel: I want to be called the Number 1> Iwtbct#1

Mehrwortmethode

Überlegen Sie sich mindestens zwei Wörter und verbinden Sie die ersten Buchstaben jedes Wortes miteinander ohne ein Leerzeichen dazwischen.
Beispiel: HerrMüllerundFrauSchneider > HMue#FSc

Hilfsmittel Passwortkarte

Die von DATEV eG entwickelte Passwortkarte ist ein Hilfsmittel für die einfache Bildung sicherer Passwörter. Ihre Anwendung ist kinderleicht:

- Wählen Sie zwei Punkte im Koordinatensystem, die sich jeweils aus einem Buchstaben und einer Zahl ergeben.
- Der erste Punkt stellt den Startpunkt dar, der zweite Punkt ist richtungsweisend.
- Vom Startpunkt aus wählen Sie einen beliebigen Weg, der in Richtung des zweiten Punktes führt. Sie folgen dem Weg so lange, bis die Mindestanzahl der benötigten Zeichen erreicht ist.

Ihr eigenes Passwortsystem

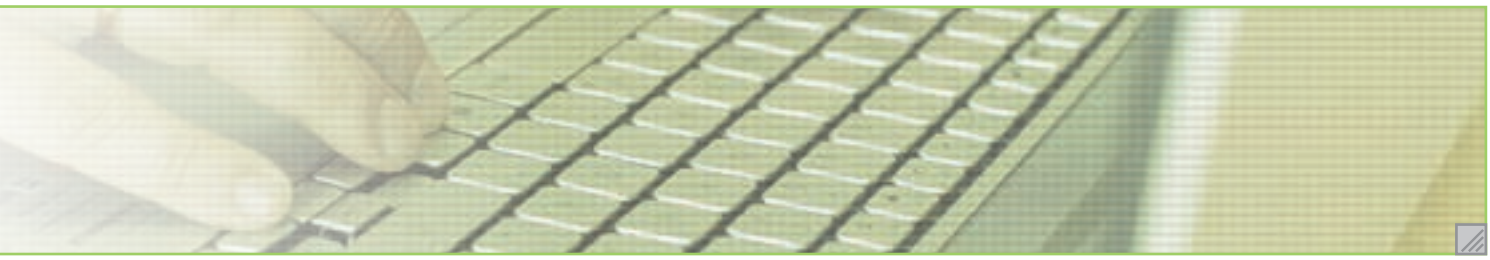
Wenn Sie viele verschiedene Accounts nutzen, wird es auch mit diesen Hilfsmitteln schwierig, alle Ihre Passwörter im Gedächtnis zu behalten. Abhilfe kann ein eigenes Passwortsystem schaffen: Kombinieren Sie ein sicheres Basispasswort, z. B. erzeugt mit einer der genannten Methoden, auf geeignete (nicht zu offensichtliche) Weise mit kontospezifischen Bestandteilen (mehr dazu unten bei unseren Hinweisen zu weiterführenden Informationen).

Verhaltensregeln

- Passwortstärke: Bilden Sie immer ein sicheres Passwort, das aus Buchstaben, Ziffern und Sonderzeichen besteht. Das Passwort sollte 8 Zeichen lang sein oder besser 10 bis 15 Zeichen enthalten.
- Geheimhaltung: Halten Sie ihr Passwort geheim und verstecken Sie es nicht an allgemein bekannten Plätzen (z. B. unter der Tastatur oder unter der Schreibtischunterlage).
- Erraten verhindern: Verwenden Sie keine personenbezogenen Daten wie den Namen Ihres Haustiers.
- Häufig ändern: Ändern Sie Ihr Passwort regelmäßig, am besten alle 6 Monate, und wenn Sie glauben, dass Ihr Passwort ausgespäht wurde.
- Kein Masterpasswort: Verwenden Sie für jede Anwendung ein anderes Passwort.

Weiterführende Informationen und Links

- Wenn Sie sich näher mit dem Thema Passwortsicherheit beschäftigen möchten, finden Sie hier weitere Informationen: **https://www.dsin-blog.de/passwortsicherheit-i-fakten-keine-mythen**.
- Die Passwortkarte als weiteres Hilfsmittel: **https://www.sicher-im-netz.de/dsin-passwortkarte**.
- Hier zeigt Ihnen ein Film, wie Sie mit richtig gewählten Passwörtern sicher durch das Netz surfen. Pfad: **www.justiz.nrw.de > Bürgerservice > Prävention > Film: Passwort Phishing**.
- Wie Sie sich mit einem individuellen Passwortsystem verschiedene Passwörter für zahlreiche Konten erstellen und merken können, lesen Sie im Artikel „Passwort-Schutz für jeden“ bei Heise Security. Pfad: Nutzen Sie auf **www.heise.de/security** die Suchfunktion mit den Stichwörtern „passwort“ und „schutz“.



4 Virenschutz und -prüfung – Basis für den persönlichen Schutz

Hintergrund und Risiken

Viren sind eine große Gefahr für Unternehmen.

Im „Fokus IT-Sicherheit 2013“[4] veröffentlichte das BSI folgende Aussage: „Die Bedrohung durch eine Vielzahl von Cyber-Gefahren hält unvermindert an. Weder für Bürger noch für Unternehmen und Behörden sinkt die Angriffslast. Nach Erkenntnissen des BSI nehmen Angreifer verstärkt die Wirtschaft ins Visier, wobei gerade auch mittelständische Unternehmen im besonderen Maße von Wirtschaftsspionage, Konkurrenzausspähung, aber auch Erpressung betroffen sind.“

Eine besondere Gefahr geht dabei von Computerviren aus. Die Bezeichnung „Virus“ bezieht sich hierbei auf die Verbreitungs- und Infektionsfunktion dieser Schadsoftware: Ein Computervirus ist laut Wikipedia „ein sich selbst verbreitendes Computerprogramm, welches sich in andere Computerprogramme einschleust und sich damit reproduziert“.

Täglich tausende neue Viren

Viren entwickeln sich in einem rasenden Tempo weiter, täglich kommen tausende neue Variationen in Umlauf. Der IT-Sicherheitsspezialist Kaspersky Lab[5] entdeckte 2013 durchschnittlich 315.000 neue Schadprogramme pro Tag, eine Steigerung von über 50 Prozent gegenüber dem Vorjahr. Nicht immer werden neue Varianten sofort nach ihrem Auftreten von allen Antivirenprogrammen erkannt; deren Hersteller liefern sich einen ständigen Wettlauf mit den Virenprogrammierern. Durch den technischen Fortschritt sind nicht nur PCs und Notebooks, sondern zunehmend auch Tablets und Smartphones betroffen.
Computerviren verbreiten sich z. B. durch direkten Datenaustausch via E-Mail oder über infizierte Seiten des Internets. Aber auch, wenn Sie keine Verbindung zum Internet haben, können Sie durch Viren gefährdet sein. Wenn Sie z. B. Datenträger mit Dritten austauschen, besteht ein Infektionsrisiko, falls Sie die Datenträger vor dem Einsatz nicht auf Viren überprüfen.

Vorbeugung ist wichtig

Regelmäßige Virenprüfungen können Schaden vermeiden.

Durch einen Virenbefall können immense Schäden entstehen, zum einen durch den längeren Ausfall wichtiger Systeme, vor allem aber auch durch das Risiko, dass wichtige Daten verloren gehen oder in die falschen Hände geraten. Viren, Trojaner und Würmer verursachen weltweit Kosten und Schäden in Milliardenhöhe. Allein in Deutschland ist jährlich von einer dreistelligen Millionensumme auszugehen – und das mit steigender Tendenz. Daher ist es äußerst wichtig und im Interesse aller, jederzeit auf einen eventuellen Virenbefall vorbereitet zu sein und u. a. eine regelmäßige Virenprüfung durchzuführen.

[4] www.bsi.bund.de
[5] www.kaspersky.com

Wenn Ihr Rechner infiziert ist

Aber was ist zu tun, wenn Ihr Computer infiziert ist? Häufige Anzeichen für einen Virenbefall sind ungewöhnliche Fehlermeldungen, verzerrte Menüs und Dialogfelder, Anwendungen funktionieren nicht korrekt, Ihr PC reagiert häufig nicht oder läuft langsamer als normal. Als Erstmaßnahme sollten Sie in diesen Fällen Ihren PC abschalten und den Zuständigen für die IT-Sicherheit oder Ihren IT-Partner über einen möglichen Virenbefall informieren. Er kennt die nächsten Schritte. Warnen Sie auch die Kollegen, mit denen Sie in letzter Zeit Daten ausgetauscht haben.

Auch wenn Sie keine solchen Anzeichen bemerken, dürfen Sie nicht davon ausgehen, dass Ihr PC auf jeden Fall sauber ist. Schadsoftware wird heute oft darauf optimiert, unauffällig zu bleiben und nicht gefunden zu werden. Vorbeugung ist daher die bei Weitem wichtigste Maßnahme.

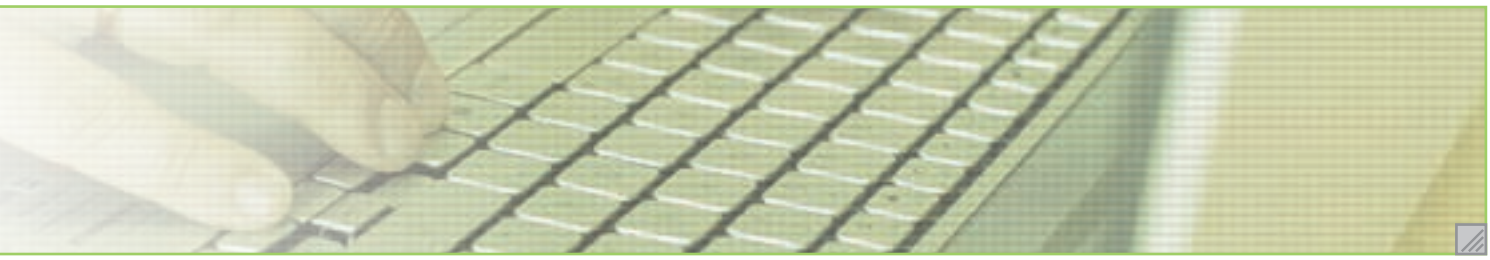
Verhaltensregeln

Handeln Sie hier gemäß dem Motto: Vorbeugen ist der beste Schutz.

- Backups: Sichern Sie Ihre Daten regelmäßig auf ein Drittmedium (z. B. externe Festplatte, USB-Stick).
- Sicherheitslücken schließen: Aktualisieren Sie alle eingesetzten Software-Produkte möglichst bald nach Erscheinen der Patches. Berichte in einschlägigen Newslettern zeigen, dass veröffentlichte Sicherheitslücken schon kurz nach Bekanntwerden ausgenützt werden.
- Virencheck: Prüfen Sie Ihren PC regelmäßig, mindestens einmal in der Woche, abhängig von Ihrem Verhalten auch öfters, auf Viren.
- Datenträger prüfen: Prüfen Sie Datenträger, die Sie von anderen erhalten, vor Verwendung auf Viren. Nutzen Sie nur auf Viren geprüfte Datenträger.
- Vertrauensfrage: Verwenden Sie nur Software aus vertrauenswürdigen Quellen.
- Im Notfall: Im Falle einer Infizierung schalten Sie Ihren PC ab und informieren Sie die „IT-Sicherheit" bzw. Ihren Chef sowie weitere möglicherweise betroffene Mitarbeiter.

Weiterführende Informationen und Links

- Weitere Informationen, wie Sie Ihren PC wirksam schützen können, finden Sie auf der Seite des BSI. Pfad: **www.bsi-fuer-buerger.de>Wie mache ich meinen PC sicher?>Schutz- und Hilfsprogramme**.
- Müssen Sie davon ausgehen, dass Ihr PC von einem Virus befallen ist, finden Sie hier auch Hilfe zur Infektionsbeseitigung. Pfad: **www.bsi-fuer-buerger.de >Wie mache ich meinen PC sicher?>Infektionsbeseitigung**.



5 E-Mail-Sicherheit – Signatur und Verschlüsselung als wichtige Elemente

Hintergrund und Risiken

Eine E-Mail ist genauso ungeschützt wie eine Postkarte.

E-Mails erleichtern die Kommunikation und den Informationsaustausch im Unternehmen und tragen zu einem effizienteren Arbeitsablauf bei. Doch wussten Sie, dass man die Vertraulichkeit einer E-Mail mit dem Versand einer offenen Postkarte vergleichen kann?

Jede unverschlüsselte E-Mail kann auf ihrem Weg durch das Internet nicht nur eingesehen, sondern auch kopiert, manipuliert oder an eine falsche Adresse versendet werden oder gar verloren gehen. Digitale Signaturen und das Verschlüsseln vertraulicher Inhalte können Ihre E-Mail-Kommunikation schützen.

Signatur und Verschlüsselung

Digitale Signaturen stellen die Echtheit des Absenders und die Integrität des Inhaltes einer E-Mail sicher. Wurde eine E-Mail während ihres Transports durch das Internet verändert, kann das der Empfänger der E-Mail erkennen. Achten Sie außerdem stets darauf, Nachrichten mit vertraulichem Inhalt oder Anhang zu verschlüsseln, um den unerwünschten Postkarteneffekt zu vermeiden. Verschlüsselte E-Mails sind nur vom Empfänger oder den Empfängern zu entschlüsseln und damit einsehbar.

Private E-Mails

Dienstliche E-Mail-Adressen und Zertifikate sollten, wenn nicht für die geschuldete Aufgabenerfüllung zwingend notwendig, von der privaten Nutzung ausgeschlossen sein. Verwenden Sie Ihre berufliche E-Mail Adresse nur für berufliche Zwecke und nicht zur Registrierung bei privat genutzten Internetdiensten (z. B. Ebay, Amazon) oder für Ihren privaten E-Mail-Verkehr. Grund hierfür sind mögliche Kontrollrechte Ihres Arbeitgebers.

Unerwünschte E-Mails

Als Spam oder Junk (englisch für „Abfall“) werden unerwünschte Nachrichten meist werbenden Inhalts bezeichnet, die dem Empfänger unverlangt zugestellt werden. Der Anteil von Spam am weltweiten E-Mail-Verkehr betrug 2013 durchschnittlich ca. 70 Prozent. Mehr als jede zehnte versandte Spam-Mail landet in Deutschland, das ist weltweit Platz 2 hinter den USA (Quelle: Kaspersky Security Bulletin Spam in 2013[6]).

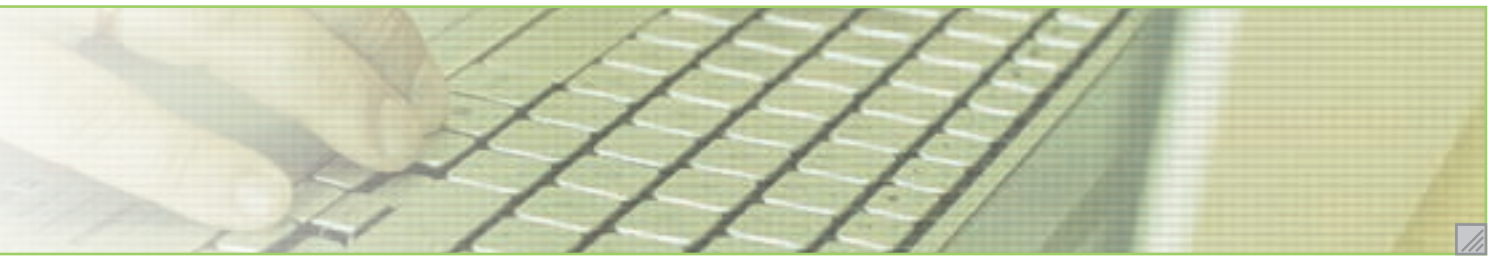
[6] www.viruslist.com

Aufgrund der enormen zusätzlich übertragenen Datenmengen (Schätzungen gehen von weltweit 100 Milliarden Junk-Nachrichten pro Tag aus) und des damit verbundenen erhöhten Aufwands verursacht Spam erhebliche Kosten. Spam-Mails können zudem Phishing-Angriffe oder virenbefallene Anhänge enthalten, die großen Schaden für Ihr Unternehmen verursachen können. Seien Sie deshalb insbesondere vorsichtig bei E-Mails, die nichts mit Ihrer beruflichen Tätigkeit zu tun haben, einen Ihnen unbekannten Absender haben und zudem in einem sehr schlechten Deutsch oder Englisch geschrieben sind. (Spams können aber auch bekannte Absender-Adressen tragen, wenn deren Accounts gehackt wurden.) Enthalten solche E-Mails zudem einen Dateianhang, öffnen Sie ihn nicht, sondern löschen Sie die E-Mail!

Die E-Mail im Rechtsverkehr

Auch E-Mails können rechtliche Folgen haben.

Auch mit einfachen E-Mails können rechtlich verbindliche Erklärungen abgegeben werden, sofern diese nicht ausdrücklich der Schriftform bedürfen. E-Mails mit „qualifizierter elektronischer Signatur" können sogar diese Voraussetzung erfüllen. Nach einer Entscheidung des LG Nürnberg-Fürth vom 7.5.2002 (Az:2 HK O 9431/01) gilt eine E-Mail im Rechtsverkehr zu dem Zeitpunkt als zugegangen, zu dem sie im elektronischen Briefkasten eingetroffen ist. Ruft der Empfänger sie nicht ab, kann er das nicht geltend machen, um etwaige Rechtsfolgen infrage zu stellen – ebenso wenig wie jemand, der seine Post nicht aus dem Briefkasten holt. Etwaige Störungen liegen ebenfalls im Risikobereich des Empfängers. Konnten also Nachrichten aus irgendeinem Grund nicht abgerufen werden, liegt die Beweislast bei ihm. Um Fristversäumnisse zu vermeiden, sollten E-Mail-Adressen, an die rechtsgeschäftliche Erklärungen geschickt werden können, arbeitstäglich kontrolliert werden.



Verhaltensregeln

- Signatur: Signieren Sie Ihre E-Mails, damit der Empfänger sicher sein kann, dass die E-Mail tatsächlich von Ihnen kommt.
- Verschlüsselung: Verschlüsseln Sie alle E-Mails mit vertraulichem Inhalt. Nutzen Sie hierzu am besten die asymmetrische Verschlüsselung. Dabei kommt ein Schlüsselpaar mit einem privaten und einem zugehörigen öffentlichen Schlüssel zum Einsatz.
- Spam-Mails: Antworten Sie nie auf Spam-Mails, öffnen Sie in der E-Mail enthaltene Links oder Anhänge nicht und löschen Sie die E-Mail umgehend.
- E-Mail-Adresse: Nutzen Sie Firmen-E-Mail-Adressen ausschließlich dienstlich. Gründe hierfür sind eventuelle inhaltliche Kontrollmöglichkeiten seitens Ihres Arbeitgebers.
- Virengefahr: Gehen Sie mit Downloads von Programmen, Bildschirmschonern und Daten-Dateien aus dem Internet sorgsam um. Sie können Trojaner oder Viren enthalten.

Weiterführende Informationen und Links

- Wenn Sie sich näher mit dem Thema „E-Mail-Sicherheit“ beschäftigen möchten, finden Sie hier weitere Informationen: Elektronischen Signatur: Pfad: **www.bsi.bund.de>Themen>elektronische Signatur**.
- Sichere E-Mail-Kommunikation und Verschlüsselung: **www.datev.de/sicherheitsleitfaden**.
- Wie Sie selbst für mehr Sicherheit sorgen und Ihre E-Mails verschlüsseln können, wird bei „Verbraucher sicher online“ erklärt. Pfad: **www.verbraucher-sicher-online.de>E-Mail>E-Mail-Verschlüsselung**.
- Vermutlich sind alle Personen, die einen E-Mail-Account haben, von Spam betroffen. Wie Sie die Zahl unerwünschter Sendungen an Sie reduzieren können, wird auf der folgenden Seite für Sie zusammengefasst. Pfad: **www.bsi-fuer-buerger.de>Welche Gefahren begegnen mir im Netz?>Spam>Hilfe für Betroffene**.

6 Mobilgeräte und Datenträger – Vermeidung von Datendiebstahl

Hintergrund und Risiken

Der Verlust mobiler Geräte birgt erhebliche Gefahren.

Im November 2012 wurde nach Angaben von Heise Security[7] aus dem Auto eines NASA-Mitarbeiters ein Notebook mit tausenden Datensätzen über Mitarbeiter und Zulieferer gestohlen. Nach Angaben der Weltraumbehörde war der gestohlene Rechner zwar mit einem Passwort geschützt, die Festplatte jedoch war unverschlüsselt. Ereignisse wie dieses sind kein Einzelfall: Vorher waren der NASA zwischen April 2009 und April 2011 bereits insgesamt 48 Rechner abhandengekommen – auf vielen davon befanden sich vertrauliche Daten.

Der Verlust oder Diebstahl von Notebooks oder auch Smartphones und Tablets birgt erhebliche Gefahren. Es entstehen nicht nur Kosten für die Wiederbeschaffung, sondern es droht auch Vertraulichkeits- oder Datenverlust, wenn dadurch fremde Personen unbefugten Zugriff auf firmeninterne Informationen erhalten.

Mobile Geräte wie Smartphones und Tablets unterstützen Sie im beruflichen und privaten Alltag mit vielen nützlichen Anwendungen wie Terminplaner, elektronischem Notizblock oder der Möglichkeit, überall von unterwegs E-Mails abrufen zu können. Doch gerade wegen ihrer Beliebtheit, ihrer kompakten Größe und dem ständigen Transport werden diese Geräte als Angriffsziele für Kriminelle immer interessanter. Das Gleiche gilt für mobile Datenträger wie USB-Sticks oder mobile Festplatten, die häufig an verschiedenen Geräten verwendet werden.

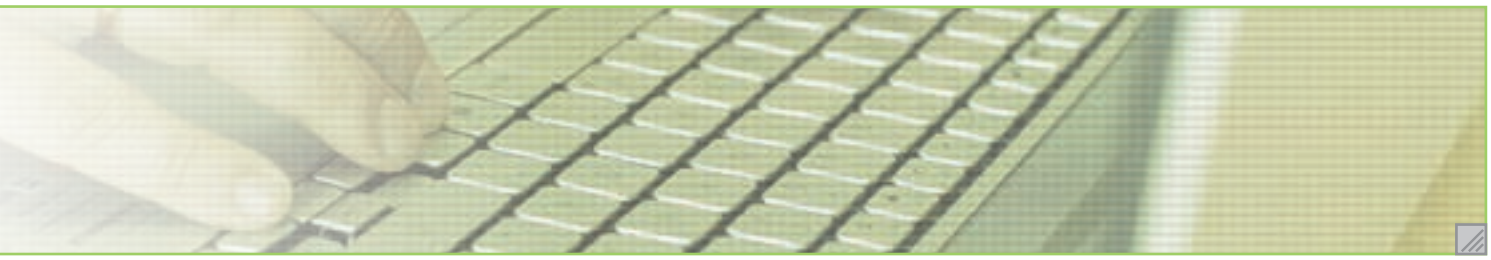
Vorsicht auch bei Datenträgern!

Bitte gehen Sie deshalb mit Ihren Mobilgeräten und Datenträgern besonders sorgsam um! Wenn das Gerät verloren geht, kann der damit verbundene Datenverlust verheerende Auswirkungen auf ein Unternehmen haben. Aus diesem Grund müssen mobile IT-Geräte noch höheren Sicherheitsstandards entsprechen als stationäre Arbeitsplatzcomputer und IT-Systeme, insbesondere wenn darauf vertrauliche Informationen gespeichert werden.

Gelegenheit macht Diebe

Geben Sie Dieben keine Chance und bewahren Sie Ihr Gerät unterwegs so sicher und unauffällig wie möglich auf. Transportieren Sie das Gerät auf Zug- oder Flugreisen im Handgepäck und auf Autofahrten von außen unsichtbar im Kofferraum.

[7] www.heise.de



Verschlüsselung der Daten

Vertrauliche Daten auf Notebooks und Smartphones sowie anderen Datenträgern sollten generell verschlüsselt werden. Notebooks und Smartphones sollten dazu mit einer Festplattenverschlüsselung ausgestattet sein. So wird sichergestellt, dass bei Verlust des Notebooks oder Smartphones nur ein materieller Schaden entsteht – die darauf gespeicherten Daten können nicht ausgespäht werden. Sollte dies nicht der Fall sein oder wenn Sie Ihre vertraulichen Daten auf einem beweglichen Datenträger, zum Beispiel auf einem USB-Stick, speichern, müssen Sie selbst für die nötige Sicherheit sorgen. Informieren Sie sich über gängige Verschlüsselungsmethoden und speichern Sie vertrauliche Daten damit ab (siehe auch Kap. 9).

Fremde Datenträger abgeben

Sollten Sie in Ihrer Firma einen fremden Datenträger, zum Beispiel einen USB-Stick oder eine Speicherkarte, finden, geben Sie ihn am besten beim Betriebsschutz/Pförtner oder bei Ihrer Führungskraft ab. Schließen Sie einen fremden Datenträger niemals an Ihrem Arbeitsplatzcomputer an, es könnten so Schadprogramme auf Ihrem Computer installiert werden.

Achten Sie auf Ihre Datenträger

Passen Sie gut auf Ihre eigenen Datenträger und Geräte auf, denn bei Verlust oder Diebstahl könnten vertrauliche Daten an Dritte gelangen. Falls doch etwas passiert: Melden Sie den Verlust Ihres Mobilgerätes, auch wenn es kurze Zeit später wieder gefunden wurde. Anschließend sollte die Integrität des Gerätes von vertrauenswürdiger Stelle sichergestellt werden.

Vorsicht geboten ist auch bei der Nutzung drahtloser Technologien wie Bluetooth oder WLAN – sie können als Einfallstor für Hacker missbraucht werden. Achten Sie zudem auf eine möglichst sichere Verwahrung. Speichern Sie Daten von mobilen Datenträgern regelmäßig auf einem Netzlaufwerk oder machen Sie Sicherungskopien auf einem weiteren Datenträger, um Datenverlust zu vermeiden.

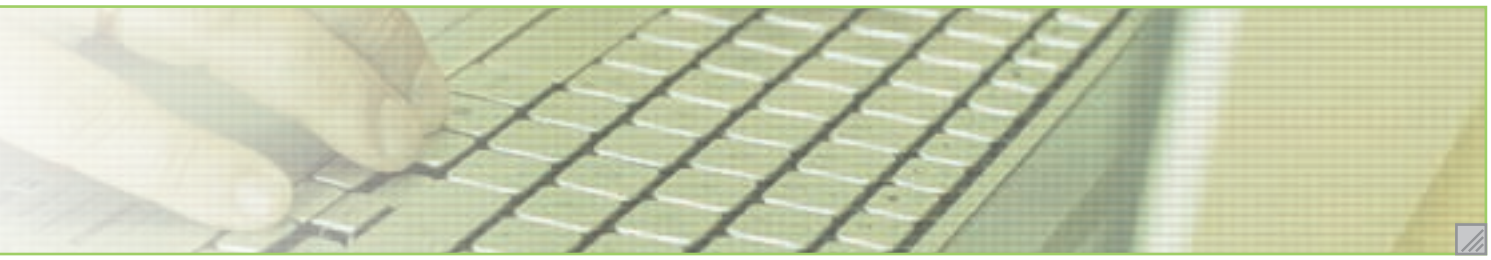
Wenn Sie ein Mobilgerät außer Betrieb nehmen, sollte sichergestellt sein, dass alle darauf gespeicherten Daten gelöscht bzw. unbrauchbar gemacht sind und das Gerät auch keine geschützten Unternehmensressourcen mehr nutzen kann.

Verhaltensregeln

- Verschlüsselung: Speichern Sie keine vertraulichen Daten unverschlüsselt auf Ihrem IT-Gerät. Bei Verlust des Gerätes kann somit nur ein materieller Schaden entstehen.
- Backups: Sichern Sie Ihre Daten regelmäßig auf einen Backup-Medium (Netzlaufwerk, weiterer Datenträger), um Datenverlust zu vermeiden
- Zugangsschutz: Schützen Sie Ihre mobilen IT-Geräte vor Zugriff von Dritten. Sperren Sie Ihr Gerät mittels eines Passwortes oder PIN-Codes und sperren Sie den Bildschirm bei Inaktivität
- Datenübertragung: Lassen Sie nur kontrollierte Datenübertragungen zu. Schalten Sie insbesondere die Bluetooth- oder WLAN-Funktion Ihres Endgerätes nur dann ein, wenn Sie diese bewusst zur Kommunikation mit bekannten Geräten und Netzen nutzen.
- Fremde Datenträger: Geben Sie fremde Datenträger bei den Kollegen der Gebäudeüberwachung (soweit vorhanden) oder bei Ihrer Führungskraft ab und schließen Sie sie niemals an Ihrem Arbeitsplatzcomputer an!
- Entsorgung: Sorgen Sie bei Außerbetriebnahme bzw. Vernichtung eines Mobilgerätes oder Datenträgers dafür, dass alle darauf gespeicherten Daten sicher gelöscht bzw. unbrauchbar sind.

Weiterführende Informationen und Links

- „Unterwegs sicher ins Netz“: Die wichtigsten Tipps zum Umgang mit Smartphones, Tablets & Co. finden Sie im DsiN-Blog unter **https://www.dsin-blog.de/unterwegs-sicher-ins-netz**.



7 Verwendung von (privater) Software – Vorgaben einhalten

Hintergrund und Risiken

Private Software am Arbeitsplatz ist ein Risikofaktor.

Mit jeder neuen Softwarekomponente, die Sie an Ihrem Arbeitsplatz installieren, kann das Sicherheitsrisiko für Ihre Firma steigen, da sie schadhaft sein oder das interne Firmennetz auf andere Weise beeinträchtigen könnte. Installieren Sie deshalb keine Software ohne Rücksprache mit Ihrem Netzwerkadministrator oder Ihrer Führungskraft. Installieren Sie insbesondere keine private Software an Ihrem Arbeitsplatz.

Sichere Installation

Wird den Sicherheitsanforderungen an eine Installation nicht Rechnung getragen, kann das fatale Folgen nach sich ziehen. So kann bei einem Einsatz ohne vorherigen Test das produktive Netz schwer beeinträchtigt werden. Zudem sollten regelmäßig Sicherheitsupdates durchgeführt werden, um sich vor Gefahren wie Hackerangriffen zu schützen – spätestens sobald Ihnen Sicherheitslücken bekannt werden.

Ungültige Lizenzen sind eine Gefahr

Die ungeregelte Installation von Software – insbesondere privater Software – erhöht nicht nur das Sicherheitsrisiko, oft sind auch dafür erforderliche Lizenzen nicht vorhanden. Eine Lizenz ist ein Nutzungsrecht, in diesem Fall das Recht zur Nutzung einer Software, das Ihnen vom Urheber (Hersteller) eingeräumt wird. Als Käufer einer kommerziellen Software erlangen Sie, der Lizenznehmer, demnach keineswegs Eigentum an dieser Software (bzw. dem Urheberrecht), sondern lediglich das Recht, die Software im Rahmen der vom Inhaber festgelegten Bedingungen und der geltenden Gesetze zu nutzen. Die konkrete Ausgestaltung dieses Nutzungsrechts liegt allein beim Softwarehersteller und schließt je nach Softwareversion oft Beschränkungen bei der Anzahl von Installationen oder Nutzern und bei der Nutzungsart (privat, geschäftlich) ein.

Ihr Chef haftet bei Lizenzverstößen und kann von Ihnen Schadenersatz fordern.

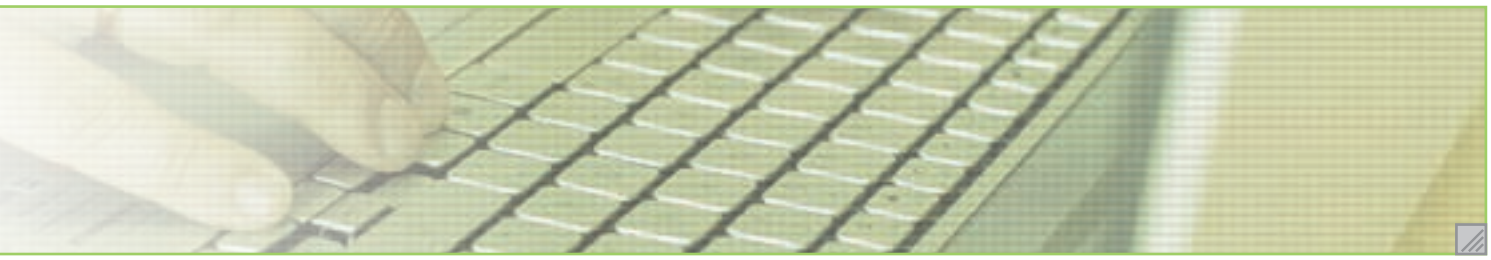
Bei einem Verstoß gegen die Lizenzbedingungen muss Ihre Firma haften und für finanzielle Schäden aufkommen. Informieren Sie sich am besten, ob in Ihrer Firma spezielle Verhaltensvorschriften zur Verwendung von Software bestehen, und wenden Sie sich im Zweifelsfall an Ihre direkte Führungskraft.

Verhaltensregeln

- Richtlinien: Informieren Sie sich, ob in Ihrer Firma Verhaltensrichtlinien zur Verwendung von Software bestehen (z. B. Verwendung privater Software, Softwareverantwortlicher), und halten Sie diese strikt ein.
- Lizenzen: Lizenzrechtliche Voraussetzungen müssen erfüllt werden. Beim Nichtvorhandensein einer gültigen Lizenz drohen hohe Straf- und Schadenersatzzahlungen.
- Updates: Installieren Sie aktuelle Sicherheitsupdates, wenn Ihnen Sicher heitslücken bekannt werden.
- Umsicht: Gehen Sie sicher, dass das produktive Netz nicht beeinträchtigt wird.

Weiterführende Informationen und Links

- Haben Sie Fragen bezüglich Open-Source-Software? Beim BSI finden Sie die Antworten. Pfad: **www.bsi-fuer-buerger.de>Wie mache ich meinen PC sicher?>Open Source Software>Fragen & Antworten**.
- Tipps und Tricks, um Ihre Software immer auf dem neuesten Stand zu halten, finden Sie unter Pfad: **www.bsi-fuer-buerger.de>Wie mache ich meinen PC sicher?>Update- und Patchmanagement**.



8 Datenverluste – Wichtige Daten regelmäßig sichern

Hintergrund und Risiken

Jedem ist das schon mal passiert: Eben haben Sie noch an Ihrem Dokument gearbeitet und jetzt ist es weg. Abstürze, technische Probleme, Softwarefehler, versehentliches Löschen oder Überschreiben – all das kann dazu führen, dass wichtige Daten nicht mehr vorhanden sind. Eine regelmäßige Sicherung auf einem externen Speichermedium ist der einzige Weg, Datenverlust nachhaltig vorzubeugen.

Der erste Blick bei Datenverlust: Papierkorb

Bei Datenverlust Ruhe bewahren.

Je länger ein Datenverlust zurückliegt, desto schwieriger ist es, die Informationen selbst zu rekonstruieren. Haben Sie ein Dokument versehentlich gelöscht, so kann ein Blick in den Papierkorb auf Ihrem PC helfen. Das ist der Ort, an den Dateien in der Standardeinstellung Ihres Betriebssystems meist beim Löschvorgang verschoben werden. Von hier aus können die gelöschten Dateien jederzeit wiederhergestellt werden. Es ist daher sinnvoll, Ihren Rechner nicht so einzurichten, dass er Daten sofort automatisch endgültig löscht.

Versehentliches Löschen vermeiden

Leider kann eine Datei auch für immer verloren gehen. Wenn Sie zum Beispiel unter Windows Dateien von einem Netzlaufwerk oder mit gedrückter STRG-Taste löschen, werden sie nicht zuerst in den Papierkorb verschoben, sondern sofort gelöscht. Auch versehentliches Überschreiben führt zu Datenverlust. Meistens passiert das, wenn Sie ein bereits bestehendes Dokument öffnen, um es als Vorlage für ein neues Dokument zu nutzen. Wenn Sie dieses Dokument ändern und dann versehentlich auf „Speichern“ klicken, wird das geänderte Dokument unter dem alten Dateinamen abgespeichert und der Inhalt des Originaldokuments ist verloren. Deshalb ist es ratsam, die Vorlage sofort unter einem anderen Dateinamen abzuspeichern. Um Fehler zu minimieren, sollten auch nur die Kollegen auf Ihre Dateien Zugriff haben, welche diese Daten zur beruflichen Aufgabenerfüllung benötigen.

Achten Sie darauf, dass Sie das Gerät immer ordnungsgemäß herunterfahren und nicht einfach ausschalten, denn auch so können Daten verloren gehen oder beschädigt werden.

Datenrettung kann sehr teuer werden

Sichern Sie alle Daten!

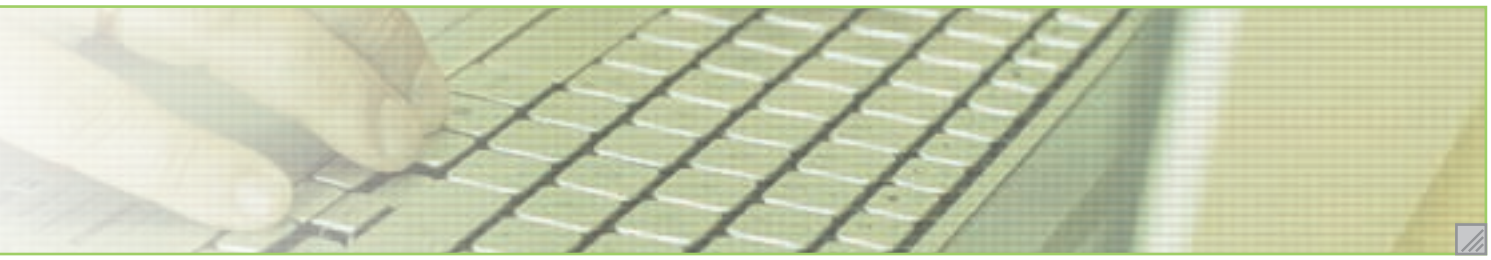
Sind Ihre Daten erst einmal verloren und lassen sich auch mit dem Datensicherungsprogramm nicht wiederherstellen, gibt es einige professionelle Programme verschiedener Softwarehersteller, die eventuell helfen können. Als letzte Möglichkeit können Fachfirmen mit speziellen Techniken versuchen, die verlorenen Daten wieder herzustellen. Das ist allerdings mit hohen Kosten verbunden und Sie selbst müssen im Einzelfall prüfen, ob sich der finanzielle Aufwand wirklich lohnt.

Regelmäßige Backups

Verlorene und nicht wiederherstellbare Daten führen zumindest zu einem Arbeitszeitausfall und bei geschäftskritischen Daten womöglich zu Schlimmerem. Um den Schaden möglichst gering zu halten, ist es notwendig, dass Sie alle betrieblichen Daten in regelmäßigen Abständen auf einem externen Datenträger sichern. Speichern Sie betriebliche Daten und Dokumente am besten von vornherein auf einem zentralen Dateiserver im Netzwerk mit zweckmäßiger Verzeichnisstruktur, entsprechend eingerichteten Zugriffsrechten (lesend oder schreibend) und automatischen Backup-Routinen.

Lokale Daten werden allerdings oftmals nicht automatisch von einer zentralen Stelle gesichert. Hier müssen Sie als Nutzer selbst tätig werden und regelmäßig Sicherungen durchführen (Kopie auf USB-Stick, Brennen einer CD bzw. DVD). Beschriften Sie unbedingt Ihre Datenträger, damit Sie später im Notfall die gesuchten Daten auch wiederfinden können. Nutzen Sie auch die in Ihren Anwendungen angebotenen Sicherungsfunktionen (z. B. automatische Speicherung von Zwischenergebnissen). Testen Sie Ihr Backup auch regelmäßig auf dessen Funktionsfähigkeit. Damit stellen Sie sicher, dass Sie Ihre Daten bei Bedarf auch wiederverwenden können.

Auch als Nutzer von Notebooks sollten Sie alle Daten auf einem Netzlaufwerk und auf mobilen Datenträgern speichern. Daten, die Sie unterwegs auf Ihrer lokalen Platte speichern, sollten am Arbeitsende auf ein Netzlaufwerk übertragen werden.



Verhaltensregeln

- Papierkorb: Leeren Sie Ihren Papierkorb auf dem PC nicht automatisch, sondern prüfen Sie in regelmäßigen Abständen, ob sich möglicherweise wichtige Daten darin befinden, die Sie aus Versehen gelöscht haben.
- Überschreiben verhindern: Speichern Sie Dateien unter einem anderen Dokumentnamen (z. B. mit Versionsnummer), wenn Sie frühere Versionen behalten möchten.
- Herunterfahren: Fahren Sie Ihren Computer immer ordnungsgemäß herunter. Ansonsten können Dateien, die gerade bearbeitet wurden, verloren gehen.
- Backups: Speichern Sie betriebliche Daten regelmäßig auf einem Netzlaufwerk und sichern Sie die Daten auf einem externen Datenträger. Testen Sie Ihr Backup auch regelmäßig auf dessen Funktionsfähigkeit. Damit stellen Sie sicher, dass Sie Ihre Daten bei Bedarf auch wiederverwenden können.
- Datenträger: Beschriften Sie Ihre Datenträger sorgfältig nach einem einheitlichen System und schützen Sie diese vor Diebstahl.

Weiterführende Informationen und Links

- Für eine intensivere Beschäftigung mit dem Thema „Datensicherung" finden Sie auf der Webseite des BSI ausführliche Informationen. Pfad: **www.bsi-fuer-buerger.de>Wie mache ich meinen PC sicher?>Datensicherung**.
- Die wichtigsten Tipps zur Datensicherung finden Sie im DsiN-Blog unter https://**www.dsin-blog.de/unterkategorien/datensicherung**.

9 Schutz von sensiblen Daten – Nur durch Verschlüsselung möglich

Hintergrund und Risiken

Wie Sie bereits gesehen haben, gibt es verschiedene Gründe, warum Verschlüsselung notwendig und auch sinnvoll sein kann. In erster Linie möchte man unbefugten Zugriff auf sensible Daten verhindern – einerseits, um die eigenen Firmendaten gegen Angriffe von außen zu schützen, andererseits, um nur den Mitarbeitern Datenzugriff zu gewähren, die diesen für die Erfüllung ihrer Aufgaben benötigen.

Hin und wieder findet ein Notebook, ein USB-Stick oder ein anderer mobiler Datenträger unfreiwillig einen neuen Besitzer, auf einem gemeinsam genutzten Computer liegen Dateien, die nicht für die Augen der Mitnutzer bestimmt sind, oder man möchte eine E-Mail mit vertraulichem Inhalt oder Anhang versenden. In all diesen Fällen kann Verschlüsselung vor einem unbefugten Zugriff schützen.

Immer mehr Unternehmen nutzen Verschlüsselungstechnologien.

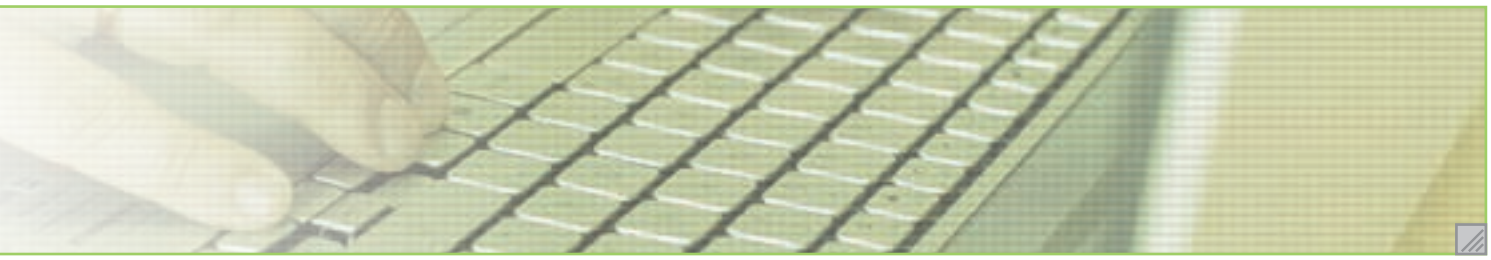
Wie BITKOM 2013[8] berichtete, sichert bereits die Mehrheit (76%) der IT-und Telekommunikationsunternehmen in Deutschland Daten oder E-Mails durch den Einsatz von Verschlüsselungstechnologien. Seit Bekanntwerden der NSA-Abhöraktionen setzen auch immer mehr Privatnutzer Verschlüsselung ein – 2013 waren es bereits 5,5 Millionen Bundesbürger (siehe weiterführende Informationen).

Wie funktioniert Verschlüsselung?

Das Grundprinzip ist denkbar einfach und existiert bereits seit der Antike: Eine Nachricht wird so verändert, dass sie für das unbefugte Auge nicht mehr verständlich ist und nur mit einem dazugehörigen Schlüssel wieder lesbar gemacht werden kann. Es werden für das Ver- und Entschlüsseln von Informationen also immer zwei Elemente benötigt: ein Schlüssel oder ein Schlüsselpaar und eine Vorschrift.

Für moderne Kommunikationstechnik gilt, dass das Ver- und Entschlüsseln von Daten bei bekanntem Schlüssel einfach und auch für unerfahrene Anwender leicht anzuwenden sein muss. Es gibt spezielle Softwarelösungen zur Verschlüsselung einzelner Dateien und Ordner oder ganzer Laufwerke sowie hardwareunterstützte Verschlüsselungsmethoden.

[8] www.bitcom.org



Was muss ich beim Einsatz von Verschlüsselung beachten?

Bei vielen Verschlüsselungslösungen werden die Daten letztlich auch nur durch ein Passwort geschützt. Wer dieses Passwort kennt, kann die verschlüsselten Daten leicht ermitteln. Es ist somit von äußerster Wichtigkeit, ein sicheres Passwort zu wählen. Wie ein sicheres Passwort aussieht und wie Sie sich dieses trotz seiner Komplexität leicht merken können, finden Sie in diesem Leitfaden im Kapitel 3 „Sicheres Passwort". Wir empfehlen die zusätzliche sichere Speicherung des Passworts bzw. Schlüssels beispielsweise auf einem externen Datenträger. So können Sie auch bei einem möglichen Verlust den weiteren Zugriff auf die Daten sicherstellen.

Auch E-Mails sollten verschlüsselt werden, wenn diese vertrauliche Daten enthalten. Eine Umfrage von BITKOM zeigt, dass im Zuge der NSA-Affäre die Zahl der Internetnutzer, die für ihre E-Mails eine Verschlüsselungssoftware nutzen, zwischen Juli und Dezember 2013 um 50 Prozent (von 6% auf insgesamt 9%) gestiegen ist. Mehr zum Thema finden Sie in diesem Leitfaden unter „E-Mail-Sicherheit" (siehe Kap. 5).

Verhaltensregeln

- **Richtlinien:** Informieren Sie sich über Verschlüsselungsvorschriften in Ihrer Firma. Gibt es bei Ihnen einen Krypto-Leitfaden? Wann müssen Sie was und wie verschlüsseln?
- **Sensible Daten:** Speichern Sie sensible Daten nur verschlüsselt auf Ihrem IT-System ab.
- **E-Mails:** Versenden Sie E-Mails mit vertraulichem Inhalt nur verschlüsselt. Wenn ein Passwort zur Entschlüsselung notwendig ist, geben Sie dieses dem Empfänger nicht per E-Mail bekannt. Wählen Sie einen unabhängigen Weg (z. B. Telefon) zur Übermittlung.
- **Up to date bleiben:** Informieren Sie sich regelmäßig über neue Verschlüsselungstechniken und verwenden Sie keine Verschlüsselungsverfahren, bei denen bekannt ist, dass mit vertretbarem Aufwand die Schutzfunktion der Verschlüsselung ausgehebelt werden kann und damit die eigentliche Nachricht lesbar ist.

Weiterführende Informationen

- Zum Thema „Daten verschlüsseln" finden Sie auf der Webseite des BSI ausführliche Informationen. Pfad: **www.bsi-fuer-buerger.de>Wie mache ich meinen PC sicher?>Datenverschlüsselung**.
- Artikel „NSA-Affäre bringt Verschlüsselung in Mode". Pfad: **www.bitkom.org >Markt&Statistik>Konsum und Nutzungsverhalten>Internet**.

Schlussappell

Bleiben Sie wachsam!

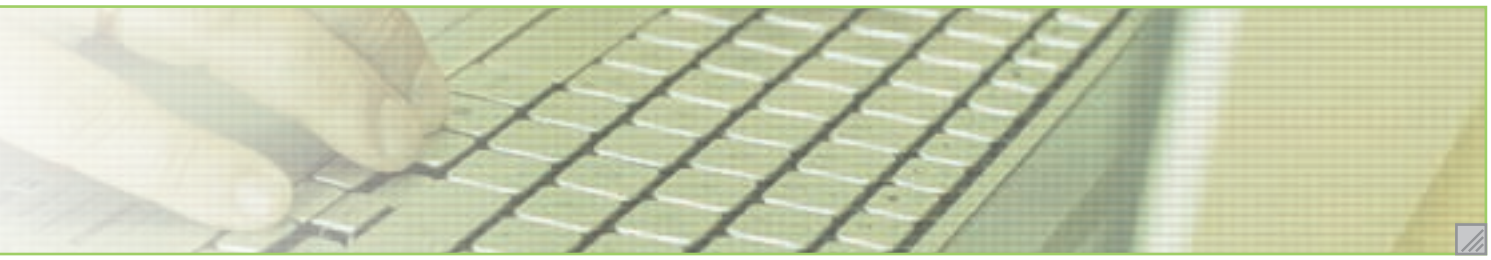
Die Daten in Ihrem Unternehmen – von geschäftlichen Dokumenten, Korrespondenzen und Kunden- oder Produktdaten bis hin zu Konstruktionsplänen oder Patentanmeldungen – sind die Basis jeder geschäftlichen Tätigkeit und damit auch Ihr „digitales Kapital".

Schützen Sie das digitale Kapital Ihres Unternehmens!

Wie Sie in diesem Leitfaden lesen konnten, ist dieses Kapital heute zahlreichen, schnell wachsenden Gefahren ausgesetzt. Helfen Sie deshalb bitte aktiv mit, die Daten Ihres Unternehmens zu beschützen! Befolgen Sie in Ihrem täglichen Umgang mit Ihren geschäftlichen Daten jederzeit die in diesem Text benannten Verhaltensregeln.

Beachten Sie: Kein Leitfaden kann alleine alle denkbaren Gefahrensituationen berücksichtigen. Deshalb gilt vor allem: Seien Sie wachsam, denken Sie mit und machen Sie sich stets die vielfältigen Informationssicherheitsrisiken bewusst, mit denen Sie im Arbeitsleben immer wieder konfrontiert sein werden.

Die Entwicklung bleibt nicht stehen – das gilt gerade auch für das Thema Informationssicherheit. Was wir heute als sicher erachten, kann morgen schon durch neue Sicherheitslücken gefährdet sein. Deshalb ist es wichtig, dass Sie sich selbst regelmäßig über neue Entwicklungen informieren. Ihr Arbeitgeber wird Sie dabei unterstützen.



Herausgeber:
Deutschland sicher im Netz e. V.
Albrechtstraße 10 a
10117 Berlin
info@sicher-im-netz.de
www.sicher-im-netz.de

2014-06-01